EL391533455US 529 Rec'd PCT/PTO 11 MAY 2000

FORM PTO-1390 (REV 12-29-99)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: PA1065US

US APPLICATION NO (If known, see 37 CFR 1 5): Unknown 09/554419

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US99/24142	14 October 1999	14 October 1998

TITLE OF INVENTION: System and Method of Sending and Receiving Secure Data with a Shared Key

APPLICANT(S) FOR DO/EO/US: Lynn D. Spraggs

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [X] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [ ] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:

    Verified Statement Claiming Small Entity Status
    Petition to Make Special & Statement in Support
    Petition Fee ($130)

526 Rec'd PCT/PTO 11 MAY 2000

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
Unknown 09/554419	PCT/US99/24142	PA1065US

17. [X] The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$840.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$670.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**

	CALCULATIONS PTO USE ONLY	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 690.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	14 - 20 =	0	X **$18.00**	$ 0.00	
Independent claims	3 - 3 =	0	X **$78.00**	$ 0.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$260.00**	$	
TOTAL OF ABOVE CALCULATIONS =				$ 690.00	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28).				$ 345.00	
SUBTOTAL =				$ 345.00	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 345.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$ 385.00	
				Amount to be refunded:	$
				charged:	$

a. [X] A check in the amount of $ 385.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

Susan Yee
Carr & Ferrell LLP
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303

Susan Yee
SIGNATURE

Susan Yee
NAME

41,388
REGISTRATION NUMBER

Atty. Dkt.No. PA1065US

Applicant: Lynn Spraggs
PCT International Serial No.: PCT/US99/24142
PCT Filed: October 14, 1999
US Serial No. Unknown
For: System and Method of Sending and Receiving Secure Data with a Shared Key

VERIFIED STATEMENT (DECLARATION) CLAIMING
SMALL ENTITY STATUS
(37 CFR 1.9 (f) and 1.27 (c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

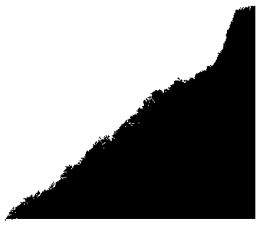
[ ] the owner of the small business concern identified below:
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN Aegis Systems Inc.
ADDRESS OF CONCERN 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.2, and reproduced in 37 CFR 1.9 (d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled "System and Method of Sending and Receiving Secure Data with a Shared Key", by inventor Lynn Spraggs, as described in

[ ] the specification filed herewith.
[X] PCT application serial no. PCT/US99/24142, filed October 14, 1999.
[ ] patent no._____, issued _____.



If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME ______________________________

ADDRESS ______________________________

[ ] INDIVIDUAL [ ] SMALL BUSINESS CONCERN [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of the Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING ASHOK MATHUR

TITLE OF PERSON IF OTHER THAN OWNER PRESIDENT

ADDRESS OF PERSON SIGNING 1101 San Antonio Road, Suite 409
Mountain View, CA 94043

SIGNATURE [signature] DATE 4/27/00

SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA WITH A SHARED KEY

Lynn D. Spraggs

BACKGROUND OF THE INVENTION

1. Field of the invention

The present invention relates generally to computer security and more specifically to allow the secure transfer and receipt of data between computers.

2. Description of the Prior Art

In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as

RSA) by a certificate authority. The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

Public key cryptography generally requires a large mathematical decomposition in order to work effectively. Generally, the length of a private key is in the order of 64 bytes. Decomposing these relatively small private keys requires considerable computational power. Public key cryptography is generally used as a one-way encryption and if a private key is changed, then everyone else that has the public key counterpart must receive a new public key.

Thus, it would be desirable to provide a system and method of securing data that is easy to use, does not require a public/private key, allows for a larger private key for more security, uses less computation power than public key cryptography, and can be used in two directions.

SUMMARY OF THE INVENTION

A system and method is provided for sending and receiving secure data. The data is secured by encrypting and decrypting the data with a key that is shared between authorized users and the server computer. As the server computer receives a user's encrypted data, the server computer decrypts the data using the user's shared key stored in a database on the server. The server computer can then process the data according to the user's instructions, this could include securely storing the data for retrieval by another user, processing the data, and/or securely sending the data to a second user by encrypting the data with the second user's shared key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a sending client transmitting secure data through a server to a receiving client over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the server computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the server computer of FIG. 2; and

FIG. 4 is a block diagram of the client computers shown in FIG. 1, in accordance with the present invention;

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module located within the client computers of FIG. 4;

FIG. 6 is a flowchart of a method illustrating how a sending client, having a shared private key, passes encrypted data to a server computer, according to the invention;

FIG. 7 is a flowchart of a method illustrating how a receiving client, having a shared private key, requests secure data from a server computer, in accordance with the invention; and

FIG. 8 is a flowchart of a method illustrating how a client, having a shared private key, passes secure data through a server computer.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private key with anyone else.

FIG. 2 is a block diagram of the server computer 100 shown in FIG. 1. Server 100 includes a CPU 202, a RAM 204, a non-volatile

memory 206, an input device 208, a display 210, and an Internet interface 212 for providing access to the Internet.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the server computer 100 of FIG. 2. The non-volatile memory 206 includes a private server key 302, a database of user private keys 304, an encrypt/decrypt engine 306, a web server engine 308 containing web page forms 310, and a secure data database 312 for storing encrypted data. The private server key 302 is known only to the server and is not shared with anyone. The database of user private keys 304 includes the private keys of registered users. Each private key of a registered user is shared only with the server and not with other users.

The encrypt/decrypt engine 306 is programmed to encrypt and decrypt data using a password or a key. Excellent results can be obtained when using the blowfish algorithm for encryption and decryption. Other types of symmetric key encryption/decryption algorithms can also be employed within the encrypt/decrypt engine 306. The computation power required to encrypt and decrypt data using a single key is much less than the computational power required in a public/private key system, therefore longer keys can be used to provide an extremely high-level of security.

FIG. 4 is a block diagram of a sending client computer 102 or a receiving client computer 104 shown in FIG. 1. Client 102, 104 includes a CPU 402, a RAM 404, a non-volatile memory 406, an input device 408, a display 410, and an Internet interface 412 for providing access to the Internet.

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 404 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page from an email sent to the clients 102, 104, and then stored on their hard drive.

FIG. 6 is a flowchart of a method illustrating how a sending client, with a shared private key, passes encrypted data to a server computer through the Internet in accordance with the invention. The process begins at step 600. The sending client establishes a session over the Internet with a suitable server by requesting a web page from the server computer at step 602. At step 604 the server sends a web page form from the web page forms database 310 to the sending client. Next at step 606 the sending client enters data into the web page along with the user's private key. At step 608 the data is encrypted with the

encrypt/decrypt engine at the sending client's computer using the user's private key and then sent to the server.

At step 610 the server receives the sending client's data and decrypts the data with the user's private key that is stored in the user private keys database 304. Then at step 612 the server re-encrypts the data using the server key 302. At step 614 the server stores the re-encrypted data in the secure data database 312 and at step 616 the process ends.

FIG. 7 is a flowchart of a method illustrating how a receiving client, having a shared private key, accesses encrypted data from the server computer through the Internet in accordance with the invention. The process begins at step 700. The receiving client establishes a session over the Internet with a suitable server by requesting the encrypted data from the server computer at step 702. At step 704 the server retrieves the encrypted data from the secure data database 312. At step 706 the server decrypts the data using the server key 302. Then at step 708 the server encrypts the data using the receiving client's private key that is stored in the user private keys database 304, and sends the encrypted data to the receiving client.

At step 710, the receiving client enters his private key, and at step 712 the encrypted data is decrypted with the receiving client's private key

using the encrypt/decrypt engine 502. At step 714 the receiving client can access or view the data, and at step 716 the process ends.

FIG. 8 is a flowchart of a method illustrating how a client, having a shared private key, passes secure data through a server computer over the Internet. This method is very similar to the process described in FIGS. 6 and 7. The process begins at step 800. A client having a private key shared with the server establishes a session over the Internet with the server by requesting a web page at step 802. At step 804 the server sends a web page form from the web page forms database 310 to the client. Next at step 806 the client enters data into the web page along with his private key shared with the server. At step 808 the data is encrypted with the encrypt/decrypt engine at the client's computer using the user's private key and then sent to the server.

At step 810 the server receives the sending client's data and decrypts the data with the user's private key that is stored in the user private keys database 304. Then at step 812 the server processes the data. This processing step can include many different types of applications including, but not limited to, storing data, calculating data, entering a stock transaction, verifying a credit card transaction, etc.

After the processing step is completed, at step 814 the server encrypts the processed data using the client's private key that is stored in the user private keys database 304 and sends the encrypted data to

the client. It is not necessary for the client to be the same client that began the process at step 802. The server can be used as an intermediary for passing and processing secure data between clients.

At step 816, the client receives the secure data and enters his private key. At step 818 the encrypted processed data is decrypted with the client's private key using the encrypt/decrypt engine 502. At step 820 the client can access or view the data, and at step 822 the process ends.

Various modifications can be made to the above described methods in order to provide a secure system and method of sending and receiving secure data with a shared key. This can be done in low-level and high-level security methods. For example, if a first user wanted to send a highly secure memo to a second person over the Internet using a screen-level encryption, the first user could write the memo at his computer, encrypt the memo and send it as an email through a server to the second user. The second user could then decrypt the email with his password and view the memo on his computer screen. The application used to decrypt and display the memo on the computer screen can be programmed so that the memo cannot ever be in a decrypted state in any file on the computer, including temporary files, but only programmed to display the decrypted memo on a computer screen. The application

could be resident on the user's computer, or it can be deployed as a Java™ applet.

I Claim:

1. A system for receiving and transmitting secure data on a server computer using a shared key, comprising:

an encrypt/decrypt engine for encrypting and decrypting data using the shared key;

a database of user shared keys for encrypting and decrypting data for a specific user.

2. The system of claim 1, further including a secure data database for storing encrypted data, and a private server key for encrypting and decrypting data stored on the server.

3. The system of claim 1, wherein the encrypt/decrypt engine uses a symmetric key encryption/decryption algorithm for encrypting and decrypting data.

4. The system of claim 1, further including a web server engine programmed to allow a user to send data securely using the encrypt/decrypt engine.

5. The system of claim 1, further including a web server engine programmed to allow a user to receive secure data using the encrypt/decrypt engine.

6. A method for receiving secure data on a server computer using a shared key, comprising the steps of:

receiving data on the server computer from a user, wherein the data is encrypted with a user's key shared between the user and the server computer;

decrypting the data with the user's key into decrypted data; and

processing the decrypted data.

7. The method of claim 6, wherein processing the decrypted data includes the steps of:

encrypting the decrypted data with a private server key; and

storing the encrypted data in a database.

8. The method of claim 7, wherein processing the decrypted data further includes the steps of:

decrypting the encrypted data with the private server key;

encrypting the data with a second user's key shared between the second user and the server computer; and

sending the encrypted data to the second user.

9. The method of claim 8, wherein the encrypted data send to the second user can only be viewed on a computer screen by the second user.

10. The method of claim 6, wherein processing the decrypted data further includes the steps of:

processing the data according to the user's instructions into processed data;

encrypting the processed data using the user's shared key; and

sending the encrypted processed data to the user.

11. A computer-readable medium comprising program instructions for receiving secure data on a server computer using a shared key, comprising the steps of:

receiving data on the server computer from a user, wherein the data is encrypted with a user's key shared between the user and the server computer;

decrypting the data with the user's key into decrypted data; and

processing the decrypted data.

12. The computer-readable medium of claim 11, wherein processing the decrypted data includes the steps of:

encrypting the decrypted data with a private server key; and

storing the encrypted data in a database.

13. The computer-readable medium of claim 12, wherein processing the decrypted data further includes the steps of:

decrypting the encrypted data with the private server key;

encrypting the data with a second user's key shared between the second user and the server computer; and

sending the encrypted data to the second user.

14. The computer-readable medium of claim 11, wherein processing the decrypted data further includes the steps of:

processing the data according to the user's instructions into processed data;

encrypting the processed data using the user's shared key; and

sending the encrypted processed data to the user.

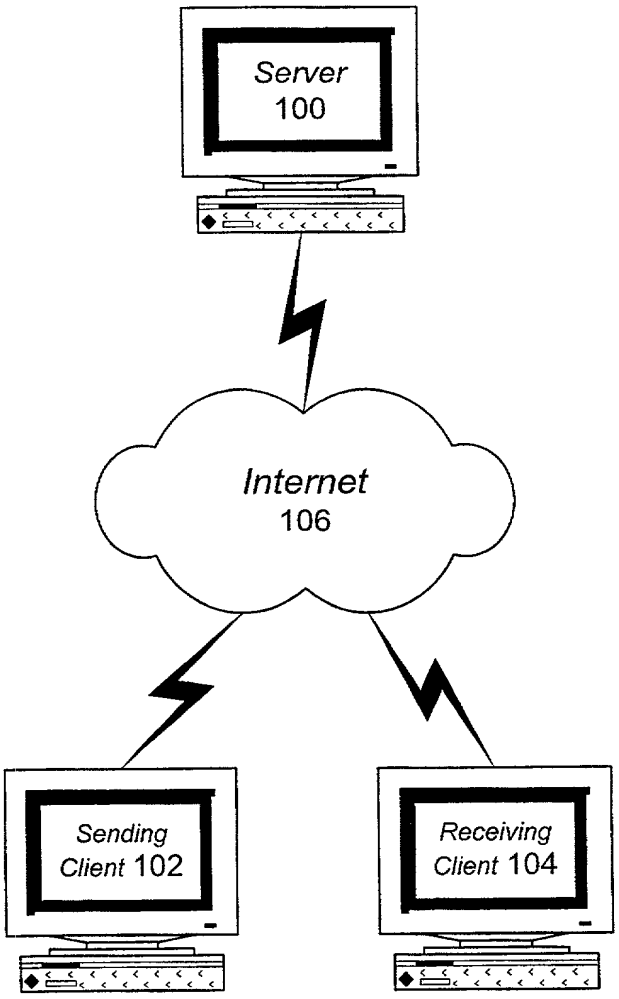

Server
100
Internet
106
Sending
Client 102
Receiving
Client 104

FIG. 1

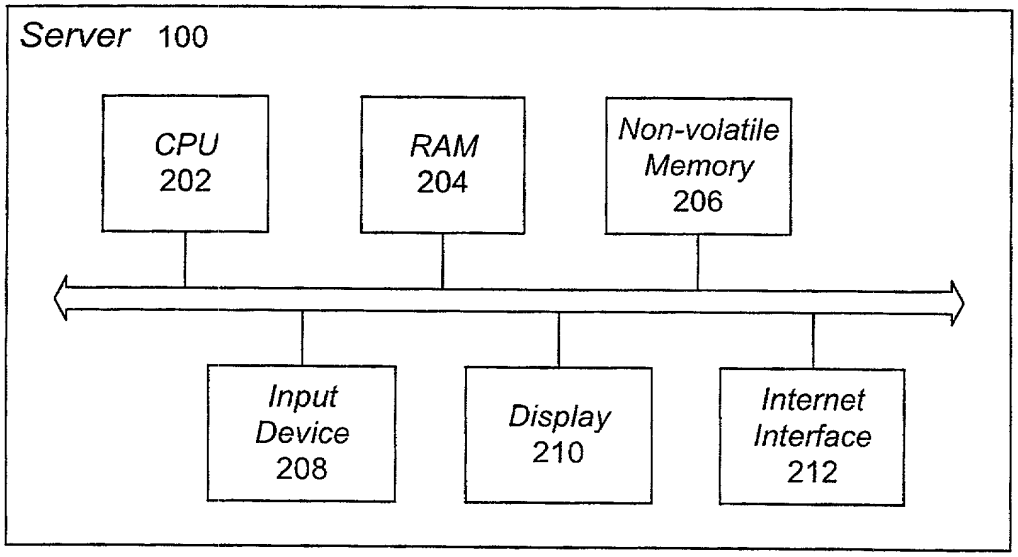

Server 100
CPU 202
RAM 204
Non-volatile Memory 206
Input Device 208
Display 210
Internet Interface 212

FIG. 2

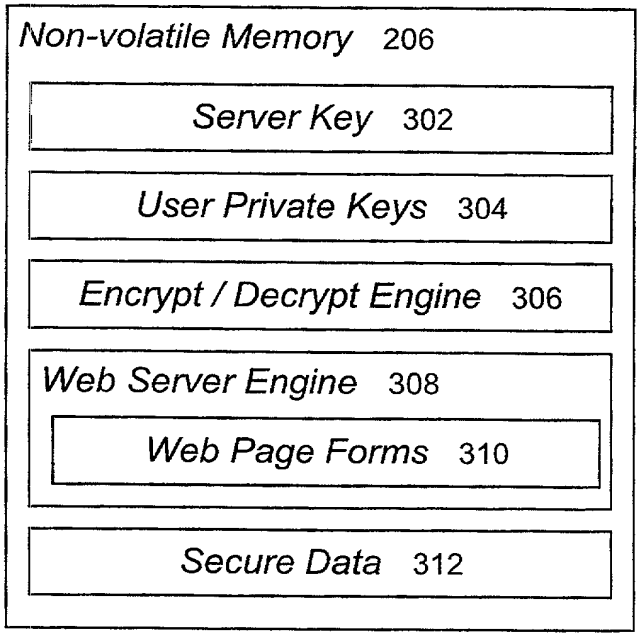

Non-volatile Memory 206
Server Key 302
User Private Keys 304
Encrypt / Decrypt Engine 306
Web Server Engine 308
Web Page Forms 310
Secure Data 312

FIG. 3

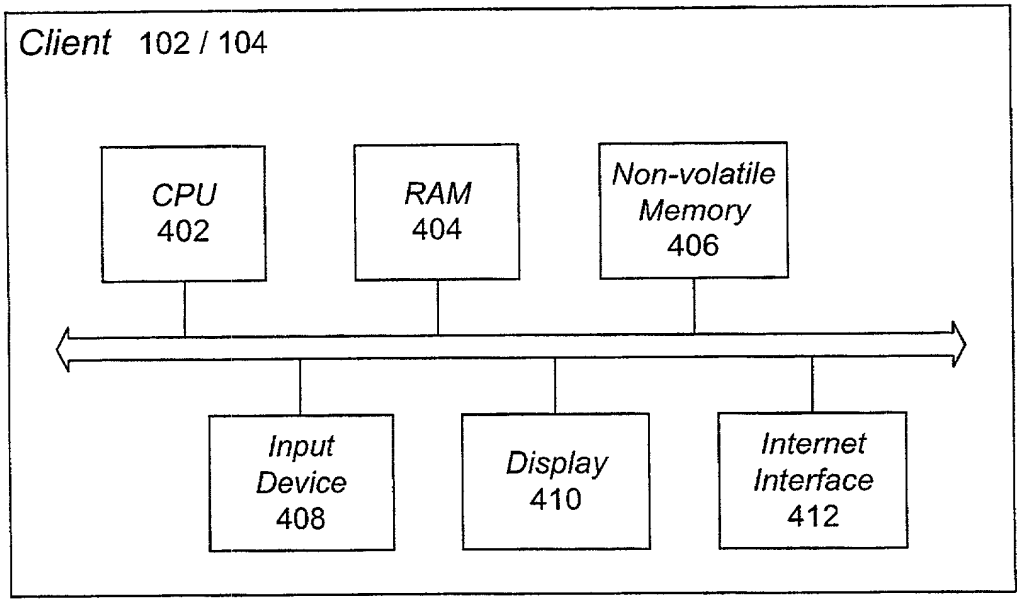

Client 102 / 104
CPU 402
RAM 404
Non-volatile Memory 406
Input Device 408
Display 410
Internet Interface 412

FIG. 4

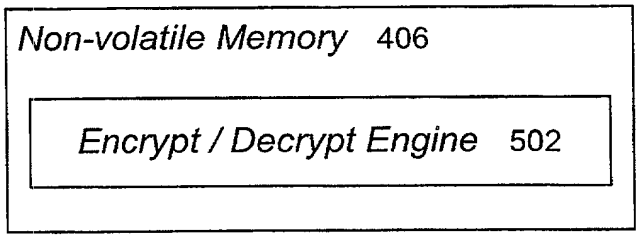

Non-volatile Memory 406
Encrypt / Decrypt Engine 502

FIG. 5

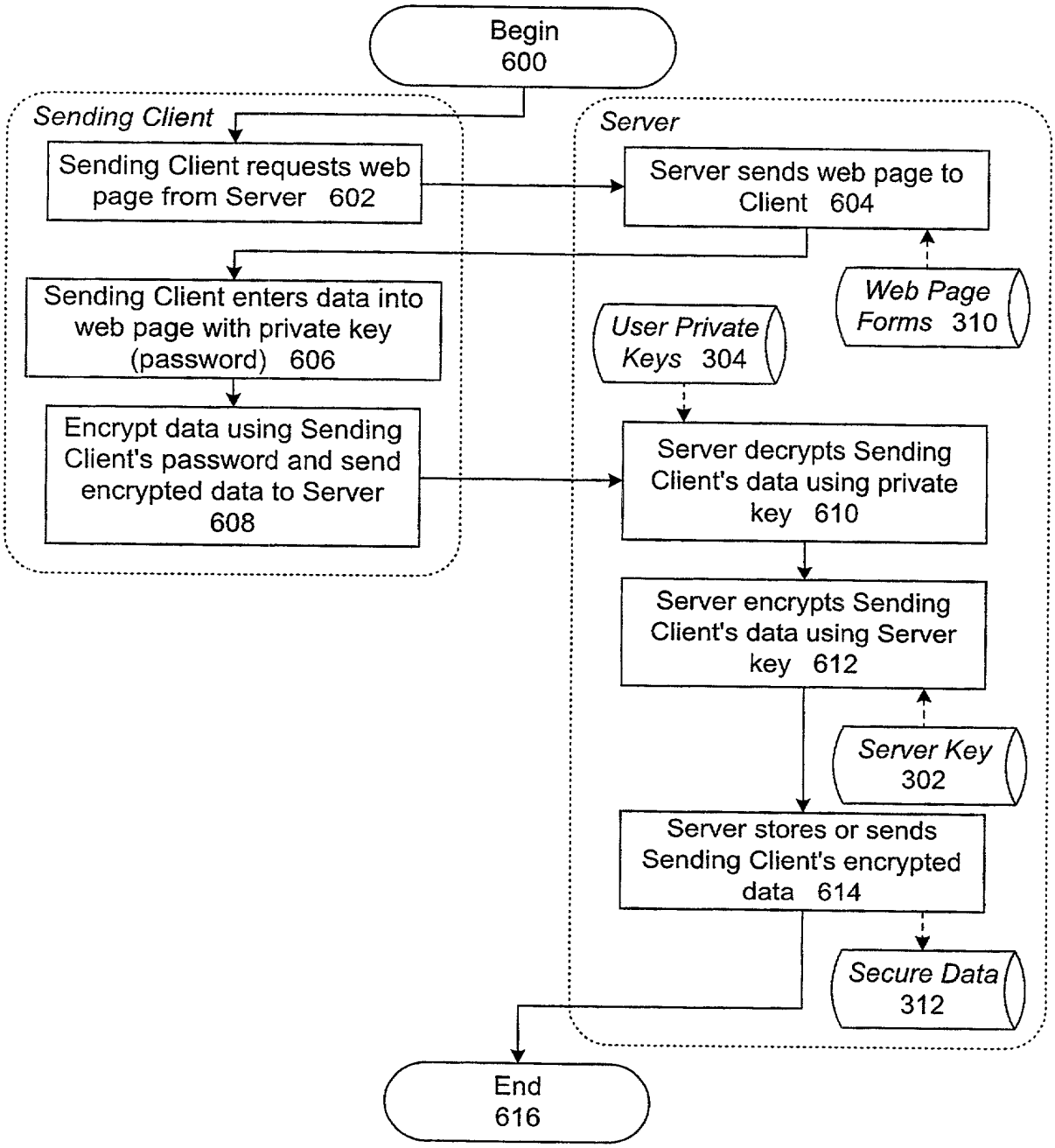

Begin
600
Sending Client
Server
Sending Client requests web page from Server 602
Server sends web page to Client 604
Web Page Forms 310
Sending Client enters data into web page with private key (password) 606
User Private Keys 304
Encrypt data using Sending Client's password and send encrypted data to Server 608
Server decrypts Sending Client's data using private key 610
Server encrypts Sending Client's data using Server key 612
Server Key 302
Server stores or sends Sending Client's encrypted data 614
Secure Data 312
End
616

FIG. 6

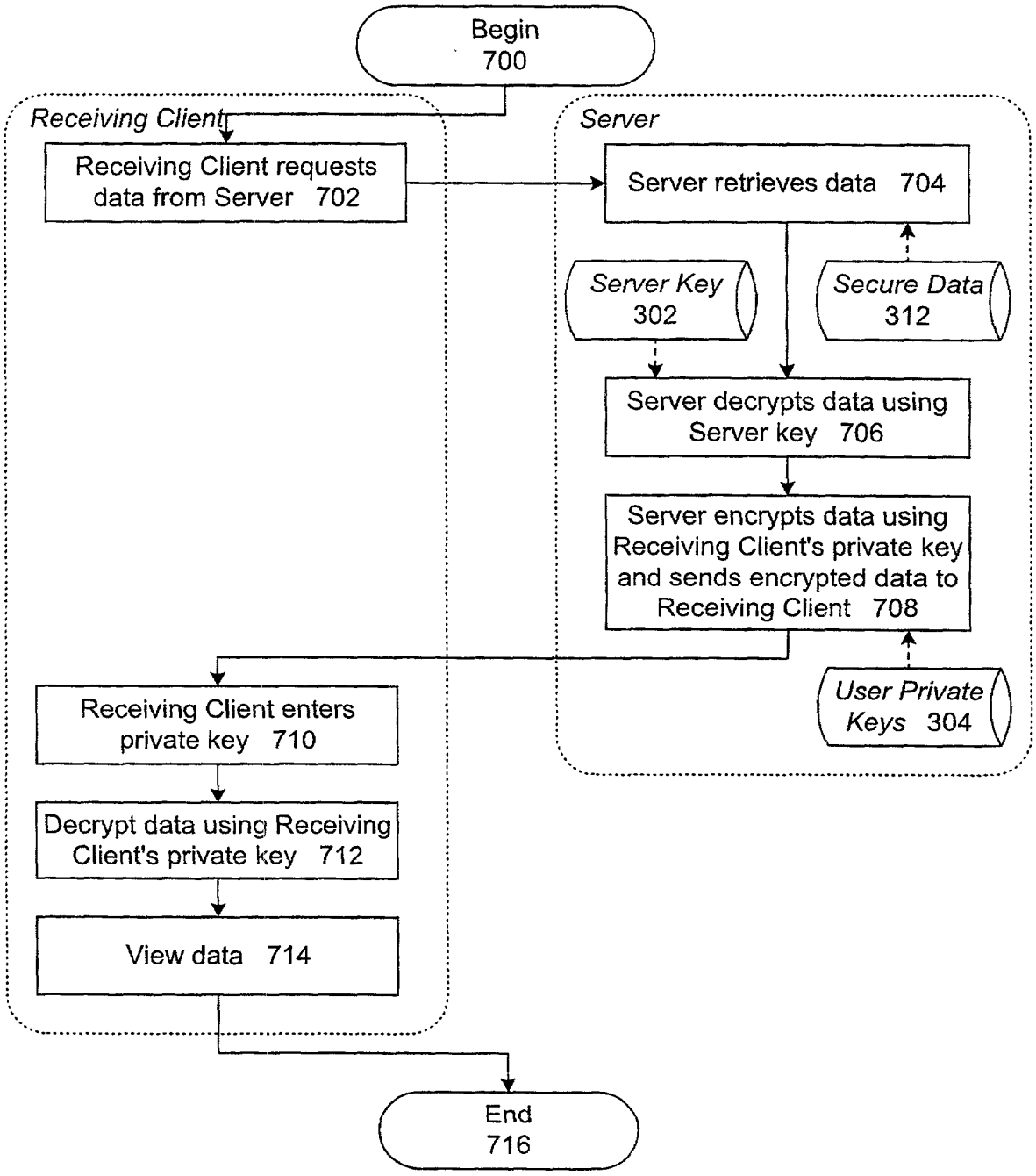

Begin
700
Receiving Client
Server
Receiving Client requests data from Server 702
Server retrieves data 704
Server Key 302
Secure Data 312
Server decrypts data using Server key 706
Server encrypts data using Receiving Client's private key and sends encrypted data to Receiving Client 708
User Private Keys 304
Receiving Client enters private key 710
Decrypt data using Receiving Client's private key 712
View data 714
End
716

FIG. 7

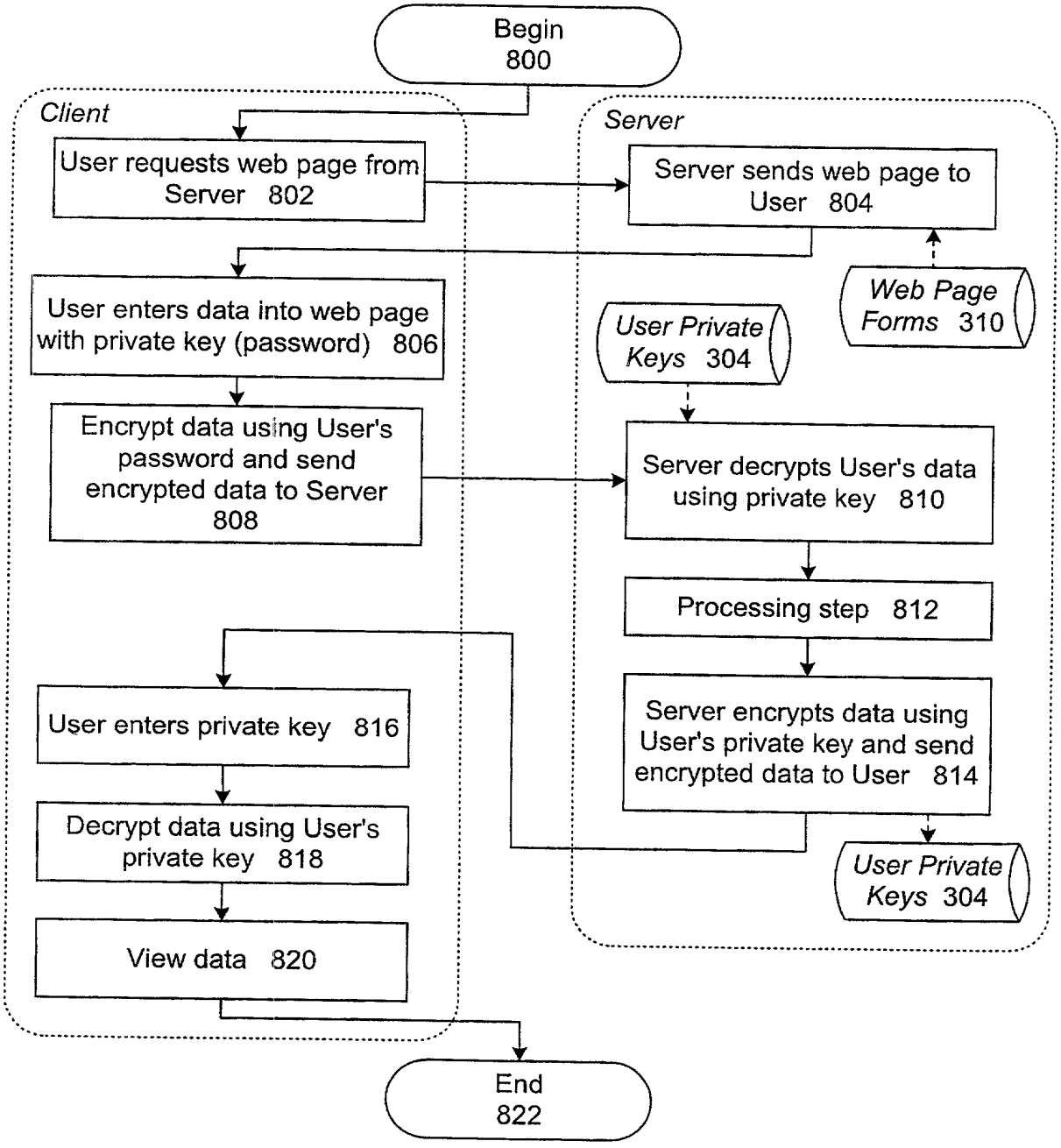

Begin
800
Client
Server
User requests web page from Server 802
Server sends web page to User 804
Web Page Forms 310
User enters data into web page with private key (password) 806
User Private Keys 304
Encrypt data using User's password and send encrypted data to Server 808
Server decrypts User's data using private key 810
Processing step 812
User enters private key 816
Server encrypts data using User's private key and send encrypted data to User 814
Decrypt data using User's private key 818
User Private Keys 304
View data 820
End
822

FIG. 8

ATTORNEY'S DOCKET NO.: PA1065US

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **"System and Method of Sending and Receiving Secure Data with a Shared Key,"** the specification of which (check one):

|__| is attached hereto.
|X| was filed on October 14, 1999
as U.S. Application No. _____
or PCT International Application No. PCT/US99/24142
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year filed)	Yes	No
(Number)	(Country)	(Day/Month/Year filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

PCT/US99/24142	October 14, 1999	Pending
(Application Number)	(Filing Date)	(Status -- patented, pending, abandoned)
(Application Number)	(Filing Date)	(Status -- patented, pending, abandoned)

POWER OF ATTORNEY: I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

John S. Ferrell, Reg. No. 34,593; J. Eppa Hite, Reg. No. 30,266;
Gregory J. Koerner, Reg. No. 38,519; Charles B. Katz, Reg. No. 36,564;
John D. Henkhaus, Reg. No. 42,656; Susan Yee, Reg. No. 41,388;
Robert Toczycki, Reg. No. 38,341 and Aaron Wininger, Reg. No. 45,229.

SEND ALL CORRESPONDENCE TO:

Aaron Wininger
CARR & FERRELL *LLP*
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
TEL: (650) 812-3400
FAX: (650) 812-3444

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor: Lynn Spraggs

Inventor's signature _____ Dated: 3/28/2000

Residence 8604 Kalavista Dr

Post Office Address Vernon B.C. CAN Citizenship Canadian